Defense Technical Information Center
Compilation Part Notice

ADP010678

TITLE: Lotus White Paper on COTS for Military
Crisis Applications

DISTRIBUTION: Approved for public release, distribution unlimited

This paper is part of the following report:

TITLE: Commercial Off-the-Shelf Products in
Defence Applications "The Ruthless Pursuit of
COTS" [l'Utilisation des produits vendus sur
etageres dans les applications militaires de
defense "l'Exploitation sans merci des produits
commerciaux"]

To order the complete compilation report, use: ADA389447

The component part is provided here to allow users access to individually authored sections
of proceedings, annals, symposia, ect. However, the component should be considered within
the context of the overall compilation report and not as a stand-alone technical report.

The following component part numbers comprise the compilation report:

ADP010659 thru ADP010682

Lotus White Paper on COTS for Military Crisis Applications

Patrick Fournery
Director of Technology
Uffe Sorensen
Director of Business & Strategies
Lotus Development S.A.
Immeuble Lotus, La Défense 6
35-41, rue du Capitaine Guynemer
92925 Paris La Défense Cedex
France

Summary: As businesses evolve to e-businesses, it is interesting to observe how the civilian requirements related to COTS software increasingly resemble the military crisis-mode requirements in terms of continuous operation (100% availability), vast scalability (Internet community), absolute reliability (transactional integrity), total security (numerous "enemies" with malicious intent in a 1B user wired community), flexible and manageable interoperability (alliances, mergers and acquisitions must be almost instantaneous and fully controlled). As COTS software vendors satisfy these civilian requirements, it will eventually facilitate military use. Inadequate software will naturally be supplanted in the marketplace by capable technologies.

"The central event of the twentieth century is the overthrow of matter. In technology, economics and the politics of nations, wealth in the form of physical resources is steadily declining in value and significance. The powers of mind are everywhere ascendant over the brute force of things. .... the most powerful corporation is .... the one with the ability to rapidly turn ideas and thinking into new products, new services and new business ! ....
In this environment, SW is not just product. It is a competitive weapon !"
Microcosm by George Gilder

Introduction

This paper is intended as an introduction to the thought-process in Lotus around Commercial Off-The-Shelf software in the context of military use.

We think that the civilian requirements placed on the software vendors actually more and more resemble demands formerly only raised in military contexts. Clearly, certain aspects of security and managing sovereignty will need specific adoption to military purposes. I deliberately write "adoption" as the fundamental COTS software is unchanged with appropriate additions and modifications for military use. A good example of this is the Lotus Domino Defense Messaging – the fundamental messaging capabilities enhanced with military grade capabilities.

In this paper we distinguish between the use of COTS software in crisis and non-crisis mode for administrative, planning, operational and conflict applications:

Administrative Applications

The use of COTS software in applications operated by mainly non-military staff dealing with non-crisis issues has clear advantages over RYO as recognized by almost all non-military organizations:

- Lower TCO – purchase price, limited education requirements around the End User Interface as most evolve towards similar paradigms, limited integration costs as standard interfaces are observed, lower maintenance cost.

- Faster implementation for quicker problem resolution.

These non-crisis mode applications are most adequately addressed by COTS software and will not be further elaborated here.

Planning Applications

Material planning and similar applications have two aspects - peace-time operation where resource planning is no different in military as compared to civilian organizations, and war-time operation where resource planning becomes highly critical. However, the same software must be used in both situations to ensure proper experience by civilians and military staff alike. Thus, requirements for this software is as for conflict applications.

Operational Applications

Peace-time operational applications, like surveillance, tracking, etc, exhibit exactly the same requirements from a military perspective as conflict applications - and indeed are also needed during war-time. Thus, requirements for this software is as for conflict applications.

Conflict Applications

RYO software has been the mainstay of these applications, although standard operating systems (UNIX derivatives, Windows NT) are increasingly the platform. The requirements which must be met by software in this category are further discussed in the following paragraphs in terms of Scalability, Availability, Reliability, Security and Interoperability.

Scalability

As civilian applications are increasingly made available to a World Wide community via the Internet - or just inside a growing enterprise conglomerate - COTS software for applications such as electronic mail, discussion databases, electronic publishing, document management, workflow, etc, must provide dramatic scalability.

Both in terms of server technology infrastructure supporting "few" to "millions" of users as well as an ability to deploy similar numbers of clients. Both when specific client side software is needed and when standardized clients (Browsers, IMAP4, etc. clients adhering to the appropriate Internet standards) are used.

Not only must a large number of users be sustained continually, however, ability to handle peek-load situations become critical (anecdotal examples are government releases of key white papers or investigatory reports creating massive peeks in traffic to a web-site).

COTS software with inadequate scalability will be supplanted in the marketplace by capable technology as the applications are being recognized as mission critical to most organizations.

From a military viewpoint, similar scalability requirements exist - both in terms of sustained load, but also in terms of concentrated periods of extreme activity. The similarity in requirements doesn't obviate the need for rigorous testing of infrastructure capacity and robustness in the military scenarios, however, the military application will not raise scalability requirements beyond for civilian use.

Availability

Outages of any particular software solution originates from one of several situations:

- Unplanned outages resulting from failure in the operational environment: These situations go beyond the particular software package, however, places requirements on the deployed operating environments and on the ability of the server software to support capabilities such as clustering and fail-over to minimize impact.

- Planned operational down-time for maintenance or other activities. Again, duplication through a clustering solution can provide increased / 100% availability.

- Unplanned outages resulting from software defects: The total impact here is directly related to the ability of the software author / provider to establish a work-around or providing a fix.

For the non-defect situations, the same Darwinistic viewpoints as expounded elsewhere leads to appropriate technologies surviving in the marketplace and being omnipresent.

For defect situations, identification and management of software defects should be understood: It is highly likely that de-facto testing of certain COTS software go beyond actual testing carried out with military RYO software due to sheer vastness of civilian deployment. Ultimately, in a critical defect situation the military becomes dependent on one of two:

1. Access to the COTS software vendor - and the ability / willingness of the vendor to provide a fix / workaround.

2. Access to the internal RYO software developer - and the ability / willingness of the IT department to provide a fix.

No clear prioritization can be done on either of these undesirable situations. However, what should also be discussed here, is the ability to even update the defunct software in a distributed network during a military conflict and other factors influencing the total availability of a particular solution.

Security

Involves two fundamental aspects: Confidentiality and authentication. Both are achieved through cryptography (symmetric and asymmetric) based on confidential and/or private/public paired keys, where the key length is the basic differentiator between civilian and military use.

Historically, the US DoD embargoed exportation of strong encryption technology outside the US, however, this trend is changing and strong encryption is being deployed for several key Internet business applications (most notably financial).

A key example to explore here is secure messaging:

• From a civilian viewpoint, messaging has evolved to require secure messages, which have been defined by the Internet Engineering Task Force (IETF) in the Secure MIME standard, allowing transmission of secure messages within the Internet, independently of the originator and cryptographic devices used on the transmitting and receiving side.

• From a military viewpoint, STANAG 4406 defines the NATO military community's protocols and standards for achieving interoperability amongst member nations. Most notably, STANAG 4406 embraces Secure MIME v3 for secure messages [v3 pending ratification by the IETF].

Lotus has been a leading provider of secure messaging solutions – signing and encrypting messages are natural features to Lotus Notes and Domino electronic mail users. A natural part of the evolution of Lotus secure mail was the complete adoption of the S/MIME v2 standard in the latest product releases.

As the provider of the most pervasive and secure messaging platform, it was natural for Lotus to also explore military messaging: Lotus introduced a special Defense Messaging Solution in the US as a natural extension to the commercial versions of Lotus Notes and Domino software.

A technologically similar solution was developed for the European market and made available as the LDDM (Lotus Domino Defense Messaging) solution with military grade security independent of the US DoD.

An essential feature in LDDM – which is also recognized as a key commercial requirement – is the ability to support country specific demands for sovereignty. Lotus provide the ability in the military augmented versions of the software to provide a owner defined and managed encryption scheme.

Generally, COTS software is evolving towards "plug-able" encryption modules – not only for specific solutions as LDDM, but generically for any application where sovereignty is essential, which today embraces almost all e-business web applications.

Reliability

With the rapid trend towards use of COTS software in e-business deployments and having mission critical transactions originate on the Internet, customers are forcing COTS software vendors to ensure transactional integrity: Civilian and military requirements towards having mission critical transactions executed once and only once are identical - and appropriately handled in COTS software today.

Interoperability

COTS software is by customer demand converging on a set of open standards, most notably Internet related standards. The effect is not only vendor independence and ability to integrate diverse applications with limited effort, but also the enablement of individual operational units to connect and interact on demand maintaining full control within each unit over the external factors that can influence the unit.

Customer demand is also forcing COTS software servers to expose their services to a common, robust programming model (most notably CORBA), which limits the investment needed in skills to utilize the services for specific tailored applications.

Conclusions

Although the specific intents of software applications for civilian versus military use are very dissimilar, the overall requirements are converging as a result of the increasing role of the Internet in connecting all businesses and consumers. We remain convinced that Lotus' COTS software with appropriate military amendments can play a significant role in military crisis applications.